(d) Providers must also ensure that customers acknowledge, agree, and warrant in writing that:

(1) The customer bears full responsibility and liability for obtaining authorization to reproduce and otherwise use the matter as proposed (including, without limitation, any trademarks, slogans, likenesses or copyrighted material contained in the image);

(2) The customer in fact has the legal authority to reproduce and otherwise use the matter as proposed; and

(3) The customer understands that images or other matter is not provided, approved, or endorsed in any way by the Postal Service.

[71 FR 65733, Nov. 9, 2006, as amended at 78 FR 44439, July 24, 2013]

§ 501.8 Postage Evidencing System test and approval.

(a) To receive Postal Service approval, each Postage Evidencing System must be submitted by the provider and evaluated by the Postal Service in accordance with the Postage Evidencing Product Submission Procedures published by PT. Copies of the current Performance Criteria may be requested via mail to the address in §501.2(g). These procedures apply to all proposed Postage Evidencing Systems regardless of whether the provider is currently authorized by the Postal Service to distribute Postage Evidencing Systems. All testing required by the Postal Service will be an expense of the provider.

(b) As provided in §501.11, the provider has a duty to report security weaknesses to the Postal Service to ensure that each approved Postage Evidencing System protects the Postal Service against loss of revenue at all times. A grant of approval of a system does not constitute an irrevocable determination that the Postal Service is satisfied with the revenue-protection capabilities of the system. After approval is granted to manufacture and/or distribute a Postage Evidencing System, no change affecting its basic features or safeguards may be made except as authorized or ordered by the Postal Service in writing.

[71 FR 65733, Nov. 9, 2006, as amended at 78 FR 44439, July 24, 2013]

§ 501.9 Demonstration or test Postage Evidencing Systems.

(a) A demonstration or test postage evidencing system is any system that produces an image that replicates a postage indicium for which the Postal Service has not received payment for postage. The following procedures must be followed to implement controls over demonstration or test Postage Evidencing Systems:

(1) A demonstration or test Postage Evidencing System may print only specimen or test indicia. A specimen or test indicia must clearly indicate that the indicia does not represent valid postage.

(2) A demonstration or test Postage Evidencing System must be recorded as such on internal provider inventory records and must be tracked by model number, serial number, and physical location.

(3) A demonstration or test Postage Evidencing System must remain under the provider's direct control. A demonstration or test Postage Evidencing System may not be left in the possession of a customer under any circumstance.

(b) All indicia printed by a demonstration or test Postage Evidencing System must be collected and destroyed daily.

§ 501.10 Postage Evidencing System modifications.

(a) An authorized provider must receive prior written approval from the manager, PT, of any and all changes made to a previously approved Postage Evidencing System. The notification must include a summary of all changes made and the provider's assessment as to the impact of those changes on the security of the Postage Evidencing System and postage funds. Upon receipt of the notification, PT will review the summary of changes and make a decision regarding the need for the following:

(1) Additional documentation.

(2) Level of test and evaluation required.

(3) Necessity for evaluation by a laboratory accredited by the National Institutes of Standards and Technology (NIST) under the National Voluntary

Laboratory Accreditation Program (NVLAP).

(b) Upon receipt and review of additional documentation and/or test results, PT will issue a written acknowledgement and/or approval of the change to the provider.

[78 FR 44439, July 24, 2013]

§ 501.11 Reporting Postage Evidencing System security weaknesses.

(a) For purposes of this section, provider refers to the Postage Evidencing System provider authorized under § 501.2 and its foreign affiliates, if any, subsidiaries, assigns, dealers, independent dealers, employees, and parent corporations.

(b) Each authorized provider of a Postage Evidencing System must notify the Postal Service within twenty-four (24) hours, upon discovery of the following:

(1) All findings or results of any testing known to the provider concerning the security or revenue protection features, capabilities, or failings of any Postage Evidencing System sold, leased, or distributed by it that has been approved for sale, lease, or distribution by the Postal Service or any foreign postal administration; or has been submitted for approval by the provider to the Postal Service or other foreign postal administration(s).

(2) All potential security weaknesses or methods of tampering with the Postage Evidencing Systems that the provider distributes of which it knows or should know and the Postage Evidencing System model subject to each such method. Potential security weaknesses include but are not limited to suspected equipment defects, suspected abuse by a customer or provider employee, suspected security breaches of the Computerized Meter Resetting System (CMRS) or databases housing confidential customer data relating to the use of Postage Evidencing Systems, occurrences outside normal performance, or any repeatable deviation from normal Postage Evidencing System performance.

(3) Cyber attacks that include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on Web sites. Cyber attacks may be carried out by third parties or insiders using techniques that range from highly sophisticated efforts to electronically circumvent network security or overwhelm Web sites to more traditional intelligence gathering and social engineering aimed at obtaining information necessary to gain access. Cyber security risk disclosures reported must adequately describe the nature of the material risks and specify how each risk affects the Postage Evidencing System.

(c) Within a time limit corresponding to the potential revenue risk to postal revenue as determined by the Postal Service, the provider must submit a written report to the Postal Service. The report must include the circumstances, proposed investigative procedure, and the anticipated completion date of the investigation. The provider must also provide periodic status reports to the Postal Service during subsequent investigation and, on completion, must submit a summary of the investigative findings.

(d) The provider must establish and adhere to timely and efficient procedures for internal reporting of potential security weaknesses and shall provide a copy of such internal reporting procedures and instructions to the Postal Service for review.

(e) Failure to comply with this section may result in suspension of approval under § 501.6 or the imposition of sanctions under § 501.12.

[71 FR 65733, Nov. 9, 2006, as amended at 77 FR 23396, Apr. 19, 2012]

§ 501.12 Administrative sanctions.

(a) An authorized Postage Evidencing System provider may be responsible to the Postal Service for revenue losses caused by failure to comply with § 501.11.

(b) The Postal Service shall determine all costs and revenue losses measured from the date that the provider knew, or should have known, of a potential security weakness, including, but not limited to, administrative and